PCT/EP03/10837

22.10.2003

BUNDESREPUBLIK DEUTSCHLAND

Prioritätsbescheinigung über die Einreichung einer Patentanmeldung

Aktenzeichen: 102 44 462.5

Anmeldetag: 24. September 2002

Anmelder/Inhaber: Siemens Aktiengesellschaft, München/DE

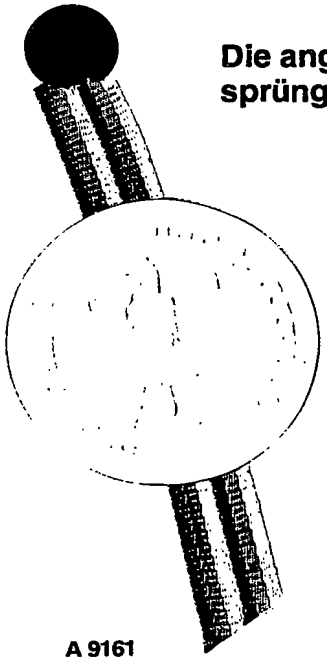
Bezeichnung: Verfahren zur Anmeldung eines mobilen Endgerätes an einem Zugangspunkt eines lokalen Kommunikationsnetzwerkes sowie Zugangspunkt und Endgerät zur Durchführung des Verfahrens

IPC: H 04 L, H 04 Q

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

München, den 16. Oktober 2003
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Faust



A 9161
08/00
EDV-L

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

Beschreibung

Verfahren zur Anmeldung eines mobilen Endgerätes an einem Zugangspunkt eines lokalen Kommunikationsnetzwerkes sowie Zugangspunkt und Endgerät zur Durchführung des Verfahrens

Die Erfindung betrifft ein Verfahren zur Anmeldung eines mobilen Endgerätes an einem Zugangspunkt eines lokalen Kommunikationsnetzwerkes gemäß Anspruch 1, einem Zugangspunkt zur Durchführung des Verfahrens gemäß Anspruch 8 sowie ein Endgerät zur Durchführung des Verfahrens gemäß Anspruch 9.

Die Verschmelzung von Informations- und Kommunikationsnetzen hat dazu geführt, dass Datenübertragungsnetze, wie Lokale Netzwerke LANs, zunehmend mit drahtlosen Zugangspunkten, sogenannten Access Points ausgestattet werden, die es erlauben, neue Netzteilnehmer, auch als Netzknoten bezeichnet, drahtlos an das LAN zu binden. Diese Entwicklung geht sogar soweit, dass zum Teil solche Netze überwiegend bzw. vollständig drahtlos Daten austauschen.

Solcherlei Netze bieten auch Raum für unberechtigte Zugriffe auf Daten innerhalb des Netzes, so dass hierfür vielerlei Ansätze zur Gewährung der Sicherheit entwickelt wurden.

Einer der Ansätze ist die Beschränkung des Datenaustausches innerhalb des Netzes auf bekannte Netzknoten, wobei ein neuer Netzknoten dadurch dem Netz bekannt gemacht wird, dass er bei einem erstmaligen Anmelden, der Erstanmeldung, Authentifizierungsdaten, zumeist Schlüssel zur Verschlüsselung von Daten bei der Übertragung, mit dem jeweiligen Zugangspunkt austauscht.

Ein Nachteil ergibt sich, wenn dieser Austausch drahtlos erfolgt. In diesem Fall kann ein möglicher Angreifer die Authentifizierungsdaten abfangen, um sich für einen unerlaubten

angriffen Endgeräte nicht verändert werden müssen, beispielsweise kann die Abwehr auch dann gewährleistet werden, wenn die Endgeräte nicht in der Lage sind, ihre Sendeleistung zu verändern.

Vorteilhafterweise wird bei einer möglichen Weiterbildung der Erfindung nach Detektieren durch den Zugangspunkt eine an das Endgerät gerichtete Signalisierung durchgeführt, welches das Endgerät veranlasst, eine zweite Sendeleistung einer zweiten Funksende-/Funkempfangseinrichtung zu senken, wobei die zweite Sendeleistung derart reduziert wird, dass ein Sende-/Empfangsvorgang nur in einem Nahfeld des Endgerätes erfolgen kann und wobei die Signalisierung vor dem Reduzieren der ersten Sendeleistung erfolgt. Hierdurch wird erreicht, dass weder die vom Zugangspunkt gesendeten Daten noch die von dem Endgerät im Rahmen des Anmeldevorgangs zu sendenden Daten von einem sich außerhalb des Nahfeldes aufhaltenden Lauscher abgefangen werden können, so dass ein Auswerten der ausgetauschten Daten gänzlich verhindert wird.

Vorzugsweise erfolgt die Signalisierung durch Übermittlung einer ersten Nachricht, die für die Angabe eines durch den Zugangspunkt ermittelten empfangenen ersten Signalpegels, insbesondere eines "Received Signal Strength Indicator" RSSI, Wertes vorgesehen ist, wobei anstelle des vorgesehenen ersten Signalpegels ein zweiter, insbesondere einen höheren Wert aufweisender, Signalpegel angegeben wird. Der Vorteil dieser Weiterbildung ist durch die hierdurch mögliche einfachere Implementierung in bereits bestehende Systeme, die zumindest teilweise eine Übertragung über Funk nutzen, gegeben, da im Wesentlichen jeder Funkkommunikationsstandard das Versenden einer derartigen Nachricht als Rückkopplungsinformation für die Quelle des jeweiligen Signals reserviert. Mit dieser Weiterbildung ist es daher möglich, dass Endgeräte ohne Änderungen das erfindungsgemäße Verfahren unterstützen können. Lediglich die Zugangspunkte müssen derart ausgestaltet sein, dass sie diese gemäß Funkkommunikationsstandards reservierte

weisen Funksende-/Funkempfangseinrichtungen neuerer Entwicklungsgenerationen, insbesondere nach dem Bluetooth-Standard funktionierende Funksende-/Funkempfangseinrichtungen, Chipsätze auf, die eine Variation der Sendeleistung in einem Endgerät erlauben.

Der erfindungsgemäße Zugangspunkt gemäß Anspruch 8 sowie das erfindungsgemäße Endgerät gemäß Anspruch 9 zeichnen sich durch Mittel zur Durchführung des Verfahrens aus, so dass das erfindungsgemäße Verfahren in den entsprechenden Geräten Unterstützung findet.

Weitere Einzelheiten und Vorteile der Erfindung werden in den Figuren 1 bis 2 erläutert. Davon zeigen

Figur 1 Darstellung eines Anordnungsszenarios, bei dem ein Versuch eines Lauschangriffs möglich wäre,

Figur 2 ein Ablaufdiagramm des erfindungsgemäßen Verfahrens bei einem Einsatz in einer Anordnung gemäß dem Szenario.

In Figur 1 ist beispielhaft eine Anordnung gezeigt, die erfindungsgemäß einen Versuch eines Lauschangriffs durch ein zum Lauschen verwendetes Endgerät LA abwehrt, wobei dies dadurch erreicht wird, dass sich ein einem lokalen Netzwerk LAN noch nicht bekanntes Endgerät, welches bei dem dargestellten Ausführungsbeispiel gemäß dem Bluetooth-Standard funktioniert, in einem ersten Funkversorgungsbereich N1 eines Zugangspunktes (Access Point) AP des lokalen Netzwerks LAN befindet.

Dieser erste Funkversorgungsbereich N1 wird von einer ersten Funksende-/Funkempfangseinrichtung TRX1 bereitgestellt, wobei eine erste Sendeleistung der ersten Funksende-/Funkempfangseinrichtung TRX1 einen von einem ersten Mikroprozessor µP1 geregelten Wert aufweist, der die Reichweite des ersten Funk-

Das Verfahren beginnt im Allgemeinen damit, dass durch den Access Point AP ein unbekanntes Endgerät PC detektiert wird und sich der Access Point AP somit in einem ersten Schritt S1 im Zustand "Unbekanntes Bluetooth Endgerät" befindet.

Ausgehend von diesem ersten Schritt S1 wird anschließend dem Bluetooth-Endgerät PC in einem folgenden zweiten Schritt S2 im Allgemeinen ein künstlich überhöhter empfangener Signalpegel signalisiert (RSSI-Wert). Künstlich überhöht bedeutet hierbei, dass im Allgemeinen nicht der tatsächlich ermittelte Signalpegelwert signalisiert wird, sondern erfindungsgemäß ein derart hoher Wert, dass das Endgerät PC seine Sendeleistung auf ein Niveau senkt, welches zu einem zweiten Funkversorgungsbereich N2 des Endgerätes PC führt, der auf ein Nahfeld begrenzt ist.

Wird das Verfahren in einem Funksystem eingesetzt, welches Endgeräte aufweist, die keine Regelung der Sendeleistung unterstützen, kann der zweite Schritt S2 ausbleiben. Alternativ ist es auch denkbar, dass der zweite Schritt S2 bewusst durchgeführt wird, selbst wenn es sich um ein Endgerät PC handeln würde, das keine Regelung unterstützt. In diesem Fall wird der Abhörschutz allein dadurch gewährleistet, dass der Zugangspunkt AP in einem dritten Schritt S3 seine Sendeleistung auf einen Wert reduziert, der den ersten Funkversorgungsbereich N1 auf ein Nahfeld begrenzt.

Unterstützt dagegen das Endgerät PC eine Regelung der Sendeleistung - wie für dieses Ausführungsbeispiel angenommen - so wird sowohl durch das Reduzieren der Sendeleistung des Zugangspunktes AP im dritten Schritt S3 als auch durch Reduzieren der Sendeleistung des Endgerätes PC in einem vierten Schritt S4 die Abwehr eines möglichen Lauschers LA gewährleistet.

Patentansprüche

1. Verfahren zur Erstanmeldung eines, insbesondere mobilen, Endgerätes (PC) an einem Zugangspunkt (AP) eines lokalen Kommunikationsnetzwerkes (LAN), dadurch gekennzeichnet, dass eine erste Sendeleistung einer ersten Funksende-/Funkempfangseinrichtung (TRX1) des Zugangspunktes (AP) nach Detektieren (S1) des Endgerätes (PC) derart reduziert wird (S3), dass ein Sende-/Empfangsvorgang nur in einem Nahfeld des Zugangspunktes (AP) erfolgen kann.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass nach Detektieren durch den Zugangspunkt eine an das Endgerät (PC) gerichtete Signalisierung durchgeführt wird, welches das Endgerät (PC) veranlasst, eine zweite Sendeleistung einer zweiten Funksende-/Funkempfangseinrichtung (TRX2) zu senken (S2), wobei die zweite Sendeleistung derart reduziert wird, dass ein Sende-/Empfangsvorgang nur in einem Nahfeld des Endgerätes (PC) erfolgen kann und wobei die Signalisierung vor dem Reduzieren der ersten Sendeleistung erfolgt.

3. Verfahren nach Anspruch 2, dadurch gekennzeichnet, dass die Signalisierung durch Übermittlung einer ersten Nachricht, die für die Angabe eines durch den Zugangspunkt (AP) ermittelten empfangenen ersten Signalpegels, insbesondere eines "Receivied Signal Strength Indicator" RSSI, Wertes vorgesehen ist (S2), erfolgt, wobei anstelle des vorgesehenen ersten Signalpegels ein zweiter, insbesondere einen höheren Wert aufweisender, Signalpegel angegeben wird.

4. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die Signalisierung (S2) eine zweite Nachricht enthält, die das Endgerät (PC) zur Ausgabe eines Hinweises an den Nutzer des Endgerätes (PC)

Zusammenfassung

Verfahren zur Anmeldung eines mobilen Endgerätes an einem Zugangspunkt eines lokalen Kommunikationsnetzwerkes sowie Zugangspunkt und Endgerät zur Durchführung des Verfahrens

Die Erfindung betrifft ein Verfahren zur Erstanmeldung eines, insbesondere mobilen, Endgerätes an einem Zugangspunkt eines lokalen Kommunikationsnetzwerkes, bei dem eine erste Sendeleistung einer ersten Funksende-/Funkempfangseinrichtung des Zugangspunktes nach Detektieren des Endgerätes derart reduziert wird, dass ein Sende-/Empfangsvorgang nur in einem Nahfeld des Zugangspunktes erfolgen kann, des Weiteren betrifft die Erfindung einen Zugangspunkt sowie ein Endgerät zur Durchführung des Verfahrens.

Figur 2

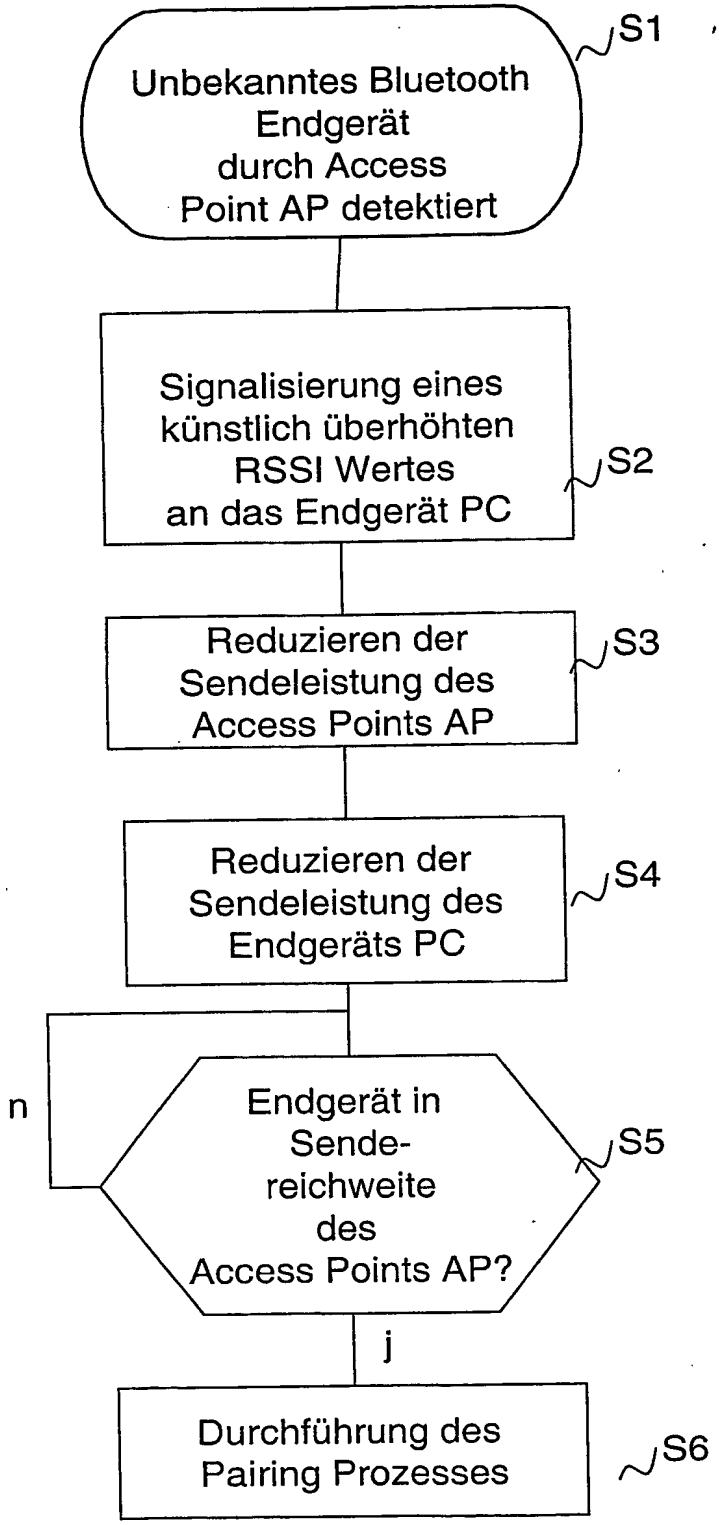

Unbekanntes Bluetooth Endgerät durch Access Point AP detektiert
S1
Signalisierung eines künstlich überhöhten RSSI Wertes an das Endgerät PC
S2
Reduzieren der Sendeleistung des Access Points AP
S3
Reduzieren der Sendeleistung des Endgeräts PC
S4
n
Endgerät in Sende-reichweite des Access Points AP?
S5
j
Durchführung des Pairing Prozesses
S6

FIG 2